Appl. No. 09/545,336
Amdt. dated January 4, 2005
Reply to Office Action of October 4, 2004

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (previously presented): A non-invasive human user identification and verification system, comprising:

a portable smart card;

a silicon-based video camera embedded within said smart card for gathering facial image data;

a digitizer integrated within said smart card for digitizing said facial image data;

non-volatile storage media for receiving and storing said digitized facial image data;

a smart-card docking station with a port for receiving said smart card and communicating said digitized image data therethrough; and

a communications interface for transmitting said stored digitized facial image data from said docking station to a central processor that is housed in a physical structure separate from said smart card, said central processor being capable of receiving and manipulating said data to produce an output signal for use in the identification and verification of said human user.

Claim 2 (previously presented): A method for the identification and verification of a human user, comprising the steps of:

capturing one or more first facial images at a remote enrollment station and digitizing said first facial images for storage in a non-volatile media within a portable smart card;

inserting said smart card with embedded video camera into a docking port; and

capturing one or more second facial images and digitizing and transmitting said second facial images from the smart card inserted in said docking port to a central processor that is housed in a physical structure separate from said smart card, said central processor being capable of receiving and comparing said first and second facial images and producing a signal indicative of recognition or non-recognition of said human user.

Claim 3 (previously presented): A human user identification and verification system, comprising:

a portable personal identification device;

a communications port adapted to receive information from the personal identification device, the communications port being external to the personal identification device;

wherein the personal identification device comprises:

a prerecorded representation of biometric data identifying an individual;

a sensor configured to capture biometric data; and

a communications interface configured to transmit information to the communications port, the information including both the prerecorded representation of biometric data identifying the individual and the biometric data captured by the sensor; and

a processor communicatively coupled to the communications port and housed in a physical structure separate from said personal identification device, the processor being configured to process the information transmitted from the personal identification device to the communications port and produce a signal indicative of whether the biometric data captured by the sensor matches the individual identified by the prerecorded representation of biometric data.

Claim 4 (previously presented): The human user identification and verification system of claim 3, wherein the personal identification device is a smart card.

Claim 5 (previously presented): The human user identification and verification system of claim 4, wherein the communications port is a docking station.

Claim 6 (previously presented): The human identification and verification system of claim 3, wherein the biometric data identifying the individual comprises facial image data and wherein the sensor is an image-capturing device.

Claim 7 (previously presented): The human identification and verification system of claim 4, wherein the biometric data identifying the individual comprises facial image data and wherein the sensor is an image-capturing device.

Claim 8 (previously presented): The human identification and verification system of claim 6, wherein the personal identification device further comprises machine-readable

storage media for storing the prerecorded representation of biometric data identifying an individual.

Claim 9 (previously presented): The human identification and verification system of claim 8, wherein the storage media comprises non-volatile memory.

Claim 10 (previously presented): The human identification and verification system of claim 3, wherein said prerecorded representation of biometric data identifying an individual comprises a plurality of facial images of the individual.

Claim 11 (previously presented): The human identification and verification system of claim 3, wherein the personal identification device is configured to acquire and store data representing a plurality of biometric characteristics of a person.

Claim 12 (previously presented): The human identification and verification system of claim 10, wherein the personal identification device is configured to automatically remove underutilized prerecorded representations of facial images.

Claim 13 (currently amended): The human identification and verification system of claim 5, wherein the docking station and sensor on the smart card are positioned to facilitate a good quality facial image capture ~~during~~ of a user during routine insertions of the smart card into the docking station.

Claim 14 (currently amended): The human identification and verification system of claim 3, ~~wherein the biometric data identifying the individual comprises data corresponding to at least two facial images,~~ wherein the sensor is an image-capturing device operable to capture at least two facial images of the individual, and wherein the processor is configured to compare the two facial images to detect motion.